

REGULATORY GUIDELINE FOR ELECTRONIC INVOICING IN NIGERIA

TABLE OF CONTENT

PART – INTRODUCTION

- 1.1. Preamble
- 1.2. Objective
- 1.3. Scope
- 1.4. Applicability
- 1.5. Definition of Terms

PART II - REGULATORY AUTHORITY

- 2.1 Responsibility of the National Information Technology Development Agency
- 2.2 Responsibility of the Federal Inland Revenue Services

PART III - PRE-ACCREDITATION OF SYSTEM INTEGRATORS

- 3.1 General Rule
- 3.2 Qualification for Accreditation
- 3.3 Technical Competence
- 3.4 Director Eligibility

PART IV - POST- ACCREDITATION OF SYSTEM INTEGRATORS

- 4.1. General rules
- 4 2. Licensing
- 4.3 Refusal to issue licence
- 4.4 Renewal of Licence
- 4.5 Termination of Licence

PART V- TECHNOLOGY REQUIREMENTS

- 5.1 General Technology Requirements
- 5.2 Data Protection

PART VI - PRE-ACCREDITATION OF ACCESS POINT PROVIDERS

- 6.1 General Rules
- 6.2 Qualification for Accreditation
- 6.3 Technical competence
- 6.4 Director Eligibility

PART VII - POST- ACCREDITATION OF ACCESS POINT PROVIDERS

- 7.1. General rules
- 7 2. Licensing
- 7.3 Refusal to issue licence
- 7.4 Renewal of Licence

- 7.5 Termination of Licence

PART VIII- TECHNOLOGY REQUIREMENTS

- 8.1 General Technology Requirements
- 8.2 Specific Technology Requirements
- 8.3 Data Protection

PART IX- PROCESSING OF E-INVOICE

- 9.1 Registration of New Users.
- 9.2 Duties of an Access Point Provider to a User

PART X- COMPLIANCE REQUIREMENTS

- 10.1 Quality of Service
- 10.2 Complaint Reporting
- 10.3 Assessment
- 10.4 Reporting
- 10.5 Audit
- 10.6 Service Availability
- 10.7 Performance Metrics

PART XI- DISCONNECTION OF SERVICE PROVIDERS

- 11.1 Guiding Principles
- 11.2 Pre-Disconnection Notice
- 11.3 Partial Disconnection

PART XII- SANCTIONS, ENFORCEMENT AND COMPENSATION

- 12.1 Enforcement and Penalty.

PART XIII- MISCELLANEOUS PROVISIONS

- 13.1 Review/Modification

APPENDICES

Appendix 1

Operator Guidelines

- a. System Integrators
- b. Access Point Providers

Appendix 2

Standardised National Schema and Naming Conventions

Overview

- a. Structure of Naming Conventions
- b. Adopted Standards for E-Invoicing
- c. HSN Code

PART I

OBJECTIVE, SCOPE AND APPLICATION OF THESE REGULATIONS

1.1 Preamble

The Federal Government of Nigeria is implementing an e-invoice system to enhance the digital transactions in Nigeria and bolster the efficiency in the administration of digital billing, account reconciliation and tax management, among other transactional components of commercial activities in Nigeria. This initiative aligns with the government's objective of improving automation and efficiency in service delivery and digitisation in Nigeria. Section 6 (C) of the enabling Act of the National Information Technology Development Agency (NITDA) vests the powers for regulation and development of electronic governance on the agency as follows:

"Develop guidelines for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper-based methods in government, commerce, education, the private and public sectors, labour, and other fields, where the use of electronic communication may improve the exchange of data and information."

In line with the above mandate, which empowers the Agency "to develop guidelines for electronic communication transaction as an alternative to paper-based methods," NITDA hereby issues these guidelines, which provide a framework for the participation of all stakeholders in the electronic invoicing process in Nigeria. The regulation will ensure the seamless and orderly development of e-invoicing technology and practice in Nigeria.

1.2 Objective

The objective of the guideline is to:

- a. To promote transparency and deepen the use of technology for e-government automation.
- b. To support the fiscal development of Nigeria for the prudent administration of government revenue to be used for development.
- c. To ensure that only qualified persons and companies who have met regulatory requirements are part of the e-invoicing process.
- d. This guideline provides a framework for implementing Business-to-Business (B2B), Business-to-Consumer (B2C), and Business-to-Government (B2G) transactions.
- e. To provide an enhanced customer-centric experience to revenue administration, improve business efficiency, and make doing business in Nigeria easier.

1.3 Scope

The guideline encompasses the entire spectrum of E-Invoicing service provisioning within Nigeria. It defines the rules and standards applicable to Access Point Providers, System Integrators and end users, ensuring a consistent and coherent use of technology in Nigeria.

1.4 Applicability

- I. These Guidelines shall apply to all privately owned companies, Federal, and State institutions, Federal Government-Owned Companies (wholly or partially owned), Business Enterprises, and individuals in Nigeria without exception.
- II. The relevant part of this guideline applies to the Invoice Access Point Providers Association.

1.5 Definition of Terms

In this Guideline, unless the context or meaning thereof otherwise requires, the following expressions shall have the meanings assigned to them in the ordinary course of businesses of the nature of this Guideline, and as herein stated:

- I. **'E-invoicing'** means a digital process that replaces paper invoices, enabling structured exchange and processing of invoices, credit, and debit notes between buyers and sellers through integrated e-invoicing solutions.
- II. **'Access Point Providers'** means an entity(ies) responsible for transmitting invoices. They also serve as the gateway that links businesses' e-invoicing solutions with the e-invoicing infrastructure mandated by the government.
- III. **'System Integrators'** means an entity(ies) that provides business software or hardware that complies with e-invoicing regulations and can securely exchange data through licensed access points.
- IV. **'User'** means an individual or business using e-invoicing services.
- V. **'Service Provider'** means 'System Integrator' or 'Access Point Provider'
- VI. **'Accreditation'** means granting permission for a licence to operate.
- VII. **'Licence'** means a substantive licence granted by the regulatory authority.
- VIII. **'Provisional License'** is a temporary licence granted pending complete application evaluation.
- IX. **'Services'** means the services the Service Provider or Regulatory Authority provides.
- X. **'Schema'** means a standardised structure and content of e-invoices.
- XI. **'Viable Minimum Product (MVP)'** is a basic version of a product developed to validate a product idea.
- XII. **'Service Level Agreement (SLA)'** means an agreement defining the level of service of an Access Point Provider to its users.
- XIII. **'Multi-factor Authentication'** means a security process requiring multiple verification factors.
- XIV. **'Tax Identification Number (TIN)'** means a unique identifier the tax authority assigns.

PART II

REGULATORY AUTHORITY

2.1 Responsibilities of the National Information Technology Development Agency

(NITDA) shall discharge the following responsibilities under these guidelines:

- I. **Accreditation:** Accrediting Service Provider to offer e-invoicing services in Nigeria, ensuring compliance with required standards and qualifications.
- II. **Technical Oversight:** Exercise regulatory control over Nigeria's technical and technology platform standards for e-invoicing and associated services.
- III. **National Standards:** Set the national standard and specifications for e-invoicing, ensuring interoperability and compatibility within the national and international e-invoicing ecosystem as provided in the Appendices to these guidelines.
- IV. **Schema Development:** In collaboration with FIRS, NITDA shall define the standardised national schema, outline the structure and content of all e-invoices within Nigeria, and promote uniformity and data integrity.
- V. **Registry:** Maintain and publish a comprehensive list of accredited Access Point Providers in Nigeria.
- VI. **Compliance Enforcement:** Enforce the Service Provider's adherence to the established national e-invoicing standards. This includes conducting regular audits and inspections to verify compliance.
- VII. **International Standard Adherence:** Where applicable, NITDA shall mandate that the Service Provider comply with relevant International E-invoicing standards to facilitate cross-border e-invoicing.
- VIII. **Data Exchange Standard:** Issue guidelines for systems and structure for exchanging e-invoicing data in Nigeria and ensure that any such transmission of invoicing data electronically outside Nigeria complies with standards as issued or ratified by NITDA.
- IX. **User Support:** Provide support and information to users, assisting them in understanding and utilising e-invoicing systems effectively.

2.2 Responsibilities of the Federal Inland Revenue Services (FIRS)

Without prejudice to the powers of the Federal Inland Revenue Service (FIRS) by all relevant laws in Nigeria, the Service shall be responsible for:

- I. **E-invoicing Platform:** Provide a centralised, accessible, and secure e-invoicing platform for Merchant Buyer Solution (MBS) that can be used by all parties involved in e-invoicing transactions within Nigeria.
- II. **Compliance Monitoring:** Ensure that the service provider adheres to the NITDA-issued standards stipulated in the appendices of this regulation during all e-invoicing platform transactions. Promptly report any deviations within a 48-hour timeframe.
- III. **Provide Education and User-Centric Platform:** Through digital literacy tools and channels, provide adequate education, explanation, and ease of use to all e-invoicing users and Nigerian citizens.

- IV. **User Support:** Offer support and information to end-users regarding e-invoicing, addressing their inquiries and concerns.

PART III

PRE-ACCREDITATION OF SYSTEM INTEGRATORS

This section outlines the general rules for obtaining accreditation as a System Integrator to operate within the E-invoicing ecosystem.

3.1 General Rules

- I. No entity shall operate as a System Integrator without prior accreditation by NITDA.
- II. NITDA shall issue a licence to each accredited System Integrator for two years, renewable on similar or new terms to be issued later.
- III. Application for accreditation shall be made to NITDA using the prescribed form.
- IV. NITDA shall initially issue a provisional licence pending technology platform examination after the demo before issuing a final licence and code.
- V. NITDA shall evaluate every technology and capability to assess capacity and expertise before licensing.
- VI. NITDA shall not accredit any company that does not submit Membership of the Invoice Access Point Providers Association.

3.2 Qualification for Accreditation

A company shall not qualify to apply for accreditation as a System Integrator unless the company complies with and meets all the following requirements:

- I. Pay a non-refundable application fee of One Million Naira only, or such other amount as NITDA may specify from time to time, payable to NITDA;
- II. Duly and properly completed accreditation form;
- III. Evidence of board resolution approving the accreditation application duly signed by the Director and Secretary of the Company;
- IV. Evidence of registration with the Corporate Affairs Commission, including the Memorandum and Article of Association, with a minimum paid-up share capital of 10 million Naira (N10,000,000.00) only.
- V. The company's Objectives shall include innovative digital technology, specifically e-invoice, in the memorandum and article of association.
- VI. Maintain a minimum of two directors who serve as company promoters.
- VII. Following Section 13 (2) (d) of the Nigerian Start-up Act 2022, Nigerians shall hold one-third of the company's shares.
- VIII. Membership of the recognised National or international Associations registered with NITDA for e-invoicing in Nigeria Platform (Where applicable)
- IX. The company must present a Viable Minimum Product (MVP) or proprietary licensed technology for e-invoicing.
- X. Detailed manuals and policies, including but not limited to operations manual, dispute resolution protocols and whistle-blowing policy.

- XI. Sworn undertaking to abide by the guideline to be notarised by the director or Company secretary.
- XII. Proof of pension contribution in line with the Pensions Act 2014.
- XIII. Evidence of ability to meet technical requirements of being an Access Point Provider.
- XIV. NITDA is expected to review and vet all documents submitted by the company and inform the company within ten (10) days of the application's status. Where there is an issue with the application, NITDA shall notify the company to rectify the defect within five (5) days and submit the application. After the resubmission, NITDA shall review the application within five days and determine its status.

3.3 Technical Competence

The Directors and management of the System Integrator must be able to fulfil their positions' responsibilities and understand the technical requirements of e-invoicing. NITDA shall take into account all relevant considerations, including but not limited to the following:

3.3.1 Board of Directors

- I. A minimum of first degree or its equivalent in any discipline plus a relevant higher degree or professional qualification;
- II. One director must have at least five (5) years of post-graduation experience, at least two (2) of which must have been in the digital technology or digital economy sector.

3.3.2 Management

- I. A minimum of first degree or its equivalent in any discipline.
- II. A minimum of two (2) years post-graduation experience, out of which at least four must have been in the digital sector;
- III. Proven skills and competencies in technology;
- IV. General knowledge of the operations of an access point provider company.
- V. Specific Knowledge of the relevant laws and regulations.

3.4 Director Eligibility

A System Integrator shall not be eligible for accreditation wherein a Director of the company is or has been:

- (1) declared bankrupt or insolvent with his bankers;
- (2) convicted of any offence involving dishonesty or fraud;
- (3) guilty of serious misconduct concerning his duties;
- (4) disqualified or suspended from practising his profession or
- (5) The Director is or has been the subject of any proceedings of a disciplinary or criminal nature or has been notified of any impending proceedings or any investigation which might lead to such proceedings. However, this provision will not apply where a person involved in such proceedings has been exonerated;

- (6) the Director has been dismissed, asked to resign from employment or a position of trust, fiduciary appointment or similar position because of questions about his honesty and integrity or
- (7) The Director has deliberately failed to inform the regulator, without reasonable cause, of the fact that their understanding of a material issue is incorrect, despite being aware of their misunderstanding or
- (8) The director ad deliberately failed to disclose the existence of falsified documents or
- (9) The director has deliberately prepared inaccurate or inappropriate documents.

PART IV

POST- ACCREDITATION OF SYSTEM INTEGRATORS

4.1 General rules

- I. NITDA may issue a provisional licence after presenting evidence of payment of the acceptance fee and subsequently issue a final licence and code to the Access Point Provider after due inspections and audits.
- II. The System Integrator must affix their license number on all products and services delivered to users to facilitate data transmission through an Access Point Provider.
- III. Comply with all other requirements as stipulated by NITDA subsequently.
- IV. Comply with all guidelines and regulations issued by NITDA.
- V. All notifications should be directed to the Director General in the prescribed format, available on the NITDA System Integrator Registration Platform.

4.2 Licensing

- I. The Provisional License will be issued for six months for commencement of service, testing, sandbox and other pre-operational procedures.
- II. The System Integrator may apply for an extension of the Provisional License for three months after the expiration of the initial term. However, no further extensions shall be granted.
- III. A System Integrator unable to secure the full licence after the extension expires must submit a fresh application for licensing under these guidelines.
- IV. The full licence to operate as a System Integrator shall be valid for two years and subject to renewal after meeting all renewal requirements.
- V. NITDA shall issue a license number, which will be found on the licence. This number will validate all products or services provided by the System Integrator.

4.3 Refusal to Issue Licence

- I. NITDA may refuse to register and issue a licence, and it shall notify the applicant in writing of its decision, stating the reason for the refusal.
- II. Where NITDA refuses to register and issue a licence due to a non-material defect in the application, it may, in the notice, require the applicant to rectify the application within 12 working days.

- III. NITDA also reserves the right to withdraw, suspend, or revoke the full or provisional licence after it has been issued if the Agency has sufficient information to make such withdrawal or suspension.
- IV. In any instance of such a licence being suspended, withdrawn, or revoked, NITDA shall provide a written basis for its action and ample opportunity for the licensee or candidate access point provider to defend itself.

4.4 Renewal of Licence

- I. The renewal of the accreditation licence shall be every two years.
- II. The approval shall be as of right where the System Integrator has done the following:
 - a. Maintain the paid-up share capital.
 - b. No outstanding or unresolved conflicts, including, but not limited to, court cases.
 - c. Meet all requirements, including Audit and clearance by all relevant regulatory authorities.

4.5 Termination of Licence

NITDA may terminate the licence of a System Integrator as follows:

- I. If the System Integrator breaches any relevant provisions or has failed to comply with a provision of the guideline.
- II. If at any point any of the accreditation requirements are unremedied for four months from the date of the termination.
- III. If there is any complaint of gross misconduct regarding the **use of** the e-invoice technology.
- IV. In the event of misuse of the data or privacy of the user or customers of the user of the System Integrator products or service or where the use of data does not comply with the provisions of NDPA 2023.
- V. Or for any other purposes that may consist of professional or gross misconduct

PART V

TECHNOLOGY REQUIREMENTS FOR SYSTEM INTEGRATORS

5.1 General Technology Requirements

The System Integrator shall comply with general technology standards issued by the Federal Inland Revenue Service :

5.2 Data Protection

- I. **Compliance with NDPA 2023**—The System Integrator must demonstrate compliance with the Nigeria Data Protection Act 2023 provisions, which regulate the lawful processing of personal data.
- II. **Data Breach**—If there is a data breach, the System Integrator must report it to NITDA and the Nigerian Data Protection Commission (NDPC) within 24 hours of the breach's

detection. Failure to report the violation will result in a fine of N1,000,000.00 and N10,000.00 for every day the Access Point Provider fails to report the violation.

- III. **Measures to Ensure Data Safety**—The Access point provider shall use best practices to ensure the safety of all data.

PART VI

PRE- ACCREDITATION OF ACCESS POINT PROVIDERS

This section outlines the general rules for obtaining accreditation as an Access Point Provider to operate within the E-invoicing ecosystem. There are two accreditation paths: The first is for Access Point Providers exclusively using the national e-invoicing platform and a further registration for Access Point Providers who intend to utilise both the national and international platforms cleared by NITDA for electronic transmission of e-invoices.

6.1 General Rules

- I. No entity shall operate as an Access Point Provider without prior accreditation by NITDA.
- II. NITDA shall issue a unique code and licence to each accredited Access Point Provider for two years, renewable on similar or new terms to be issued later.
- III. Application for accreditation shall be made to NITDA using the prescribed form.
- IV. NITDA shall initially issue a provisional licence and code pending technology platform examination after the demo before issuing a final licence and code.
- V. NITDA shall evaluate every platform to assess security, user-centricity, and ease of use before granting a full licence.
- VI. Nitda shall not accredit any company that does not submit Membership of the National Association of E-invoicing platform in Nigeria,

6.2 Qualification for Accreditation

A company shall not qualify to apply for accreditation as an Access Point Provider unless the company complies and meets all the following requirements:

- I. Pay a non-refundable application fee of One Million Naira only, or such other amount as NITDA may specify from time to time, payable to NITDA;
- II. Duly and properly completed accreditation form;
- III. Evidence of board resolution approving the accreditation application duly signed by the Director and Secretary of the Company;
- IV. Evidence of registration with the Corporate Affairs Commission, including the Memorandum and Article of Association, with a minimum paid-up share capital of 100 million Naira only.
- V. The company's Objectives shall include innovative digital technology, specifically e-invoice, in the memorandum and article of association.
- VI. Maintain a minimum of three directors who serve as company promoters.
- VII. Following Section 13 (2) (d) of the Nigerian Start-up Act 2022, Nigerians shall hold one-third of the company's shares.

- VIII. Membership of the recognised National or international Associations registered with NITDA for e-invoicing in Nigeria Platform (Where applicable)
- IX. The company must present a Viable Minimum Product (MVP) or proprietary licensed technology for e-invoicing.
- X. Concise business plan or feasibility report in the prescribed format, which shall, at a minimum, include:
 - a. Objectives of the company;
 - b. Justification for the application;
 - c. Organisational structure, including the operation and technical units, responsibilities and reporting relationships;
 - d. Details of proposed management staff in charge of the operation and technical units;
 - e. A comprehensive plan for commencing operations with milestones and timelines. An information security, data protection, and business continuity plan.
- XI. Detailed manuals and policies, including but not limited to operations manual, dispute resolution protocols and whistle-blowing policy.
- XII. Sworn undertaking to abide by the guideline to be notarized by the director or Company secretary.
- XIII. Proof of pension contribution in line with the Pensions Act 2014.
- XIV. Evidence of ability to meet technical requirements of being an Access Point Provider.
- XV. NITDA is expected to review and vet all documents submitted by the company and inform the company within ten (10) days of the application's status. Where there is an issue with the application, NITDA shall notify the company to rectify the defect within five (5) days and submit the application. After the resubmission, NITDA shall review the application within five days and determine its status.

6.3 Technical Competence

The Directors and management of the Access Point Provider must be able to fulfil their positions' responsibilities and understand the technical requirements of e-invoicing. NITDA shall take into account all relevant considerations, including but not limited to the following:

6.3.1 Board of Directors

- I. A minimum of first degree or its equivalent in any discipline plus a relevant higher degree or professional qualification;
- II. One director must have at least ten (10) years of post-graduation experience, at least ten of which must have been in the digital technology or digital economy sector.
- III. One director must also have at least three (3) years of senior manager experience or equivalent experience.

6.3.2 Management

- I. A minimum of first degree or its equivalent in any discipline.

- II. A minimum of five years post-graduation experience, out of which at least four must have been in the digital sector;
- III. At least two (2) directors must have senior management level experience.
- IV. Proven skills and competencies in technology;
- V. General knowledge of the operations of an access point provider company.
- VI. Specific Knowledge of the relevant laws and regulations.

6.4 Director Eligibility

An Access Point Provider shall not be eligible for accreditation wherein a Director of the company is or has been:

- (1) declared bankrupt or insolvent with his bankers;
- (2) convicted of any offence involving dishonesty or fraud;
- (3) guilty of serious misconduct concerning his duties;
- (4) disqualified or suspended from practising his profession or
- (5) The Director is or has been the subject of any proceedings of a disciplinary or criminal nature or has been notified of any impending proceedings or any investigation which might lead to such proceedings. However, this provision will not apply where a person involved in such proceedings has been exonerated;
- (6) the Director has been dismissed, asked to resign from employment or a position of trust, fiduciary appointment or similar position because of questions about his honesty and integrity or
- (7) The Director has deliberately failed to inform the regulator, without reasonable cause, of the fact that their understanding of a material issue is incorrect, despite being aware of their misunderstanding or
- (8) The director ad deliberately failed to disclose the existence of falsified documents or
- (9) The director has deliberately prepared inaccurate or inappropriate documents.

PART VII

POST- POST-ACCREDITATION OF ACCESS POINT PROVIDERS

7.1 General rules

- I. NITDA may issue a provisional licence after presenting evidence of payment of the acceptance fee and subsequently issue a final licence and code to the Access Point Provider after due inspections and audits.
- II. The Access Point Provider shall present the code to the FIRS for onboarding on the National E-invoicing Platform.
- III. Comply with all other requirements as stipulated by NITDA subsequently.
- IV. Comply with all guidelines and regulations issued by NITDA.
- V. Notify NITDA upon commencement of operations.
- VI. Notify NITDA when there are composition and operations changes within 48 hours.
- VII. The Access Point Provider and the User shall execute a Service Level Agreement (SLA) outlining both parties' performance standards and responsibilities in the e-

invoicing process. The SLA may be reviewed annually at both parties' discretion and updated as necessary to reflect service requirements or performance changes.

- VIII. All notifications should be directed to the Director General in the prescribed format, available on the NITDA Access Point Provider Registration Platform.

7.2 Licensing

- I. The Provisional License will be issued for six months for commencement of service, testing, sandbox and other pre-operational procedures.
- II. The Access Point Provider shall notify the Director General of its readiness to provide service at any time within six months of issuing the Provisional License.
- III. The Access Point Provider may apply for an extension of the Provisional License for three months after the expiration of the initial term. However, no further extensions shall be granted.
- IV. An access Point Provider unable to secure the full licence after the extension expires must submit a fresh application for licensing under these guidelines.
- V. The full licence to operate as an Access Point Provider shall be valid for two years and subject to renewal after meeting all renewal requirements.
- VI. NITDA shall issue a code alongside the licence to onboard the Access point provider on the National E-invoicing platform.
- VII. Access point providers qualify to provide all services provided by system integrators.

7.3 Refusal to Issue Licence

- I. NITDA may refuse to register and issue a licence, and it shall notify the applicant in writing of its decision, stating the reason for the refusal.
- II. Where NITDA refuses to register and issue a licence due to a non-material defect in the application, it may, in the notice, require the applicant to rectify the application within 12 working days.
- III. NITDA also reserves the right to withdraw, suspend, or revoke the full or provisional licence after it has been issued if the Agency has sufficient information to act accordingly.
- IV. In any instance of such a licence being suspended, withdrawn, or revoked, NITDA shall provide a written basis for its action and ample opportunity for the licensee or candidate access point provider to defend itself.

7.4 Renewal of Licence

- I. The renewal of the accreditation licence shall be every two years.
- II. The approval shall be as of right where the Access Point Provider has done the following:
 - a. Maintain the paid-up share capital.
 - b. No outstanding or unresolved conflicts, including, but not limited to, court cases.
 - c. Meet all requirements, including Audit and clearance by all relevant regulatory authorities.

7.5 Termination of Licence

NITDA may terminate the licence of an Access Point Provider as follows:

- I. If the Access Point Provider breaches any relevant provisions or has failed to comply with a provision of the guideline.
- II. If at any point any of the accreditation requirements are unremedied for four months from the date of the termination.
- III. If there is any complaint of gross misconduct regarding the **use of** the e-invoice technology.
- IV. In the event of misuse of the data collected by the Access Point Provider or where the use of data does not comply with the provisions of NDPA 2023.
- V. Or for any other purposes that may consist of professional or gross misconduct

PART VIII

TECHNOLOGY REQUIREMENTS FOR ACCESS POINT PROVIDERS

8.1 General Technology Requirements

The Access Point Provider shall comply with general technology standards issued by the Federal Inland Revenue Service and ensure that:

- I. End- User transaction information is transmitted securely as required in the technical documentation (docs) ;
- II. The e-invoice technology deployed must comprise a set of interoperable infrastructures;
- III. The e-invoice technology deployed must ensure that end users get the E-invoice after a successful transaction;
- IV. Immediate notification shall be mandatory if an E-invoice transaction fails;
- V. The Access Point Provider shall implement adequate measures to mitigate all risks arising from deploying and using its Information Technology architecture.

8.2 Specific Technology Requirements

The Access Point Provider shall comply with specific technology standards regarding E-invoicing. The Access Point Provider shall ensure that:

- I. All end users must use multi-factor authentication to ensure the E-invoicing process is safe for all parties.
- II. Encryption is mandatory for all e-invoicing Access Point Providers, and all data exchanges in the e-invoice process shall be encrypted.
- III. Access Point Providers must use a standardised national schema for transmitting E-invoice to ensure consistency and accuracy.
- IV. The standardised national schema shall include the following:
 - a. Invoice date;
 - b. Business name and address;
 - c. Customer's business name and address;
 - d. Unique invoice number;

- e. Payment due and the terms, including payment method;
- f. Description of the services provided.

8.3 Data Protection

- I. **Compliance with NDPA 2023**—The Access Point Provider must demonstrate compliance with the Nigeria Data Protection Act 2023 provisions, which regulate the lawful processing of personal data.
- II. **Data Breach**—If there is a data breach, the Access Point provider must report it to NITDA and the Nigerian Data Protection Commission (NDPC) within 24 hours of the breach's detection. Failure to report the violation will result in a fine of N1,000,000.00 and N10,000.00 for every day the Access Point Provider fails to report the violation.
- III. **Measures to Ensure Data Safety**—The Access point provider shall use best practices to ensure the safety of all data.

PART IX

PROCESSING OF E-INVOICE

9.1 Registration of New Users

- I. New Users are required to acquire a Tax Identification Number (TIN) from the FIRS.
- II. The Access Point Provider shall issue a code to the new User, which will be generated on the FIRS platform. The code will be the user's standard identification within the e-invoicing system.
- III. The new user can use any System Integrator product or service and any Access Point Provider to provide e-invoicing services.
- IV. If a new user has multiple branches of the same business at different locations, the user may create multiple sub-users under his account.
- V. A non-resident who makes taxable supplies to Nigeria must obtain a Tax Identification Number (TIN) and include value-added tax (VAT) on its--invoice for all taxable supplies.

9.2 Duties of an Access Point Provider to a User

- I. Create and maintain the connectivity gateways that function as access nodes on the e-invoicing network.
- II. Comply with the standard issued by NITDA and the tax authority FIRS.
- III. Comply with the e-invoicing standards set by the International Organisation (Where applicable).
- IV. Authenticate users through a dedicated authentication mechanism.
- V. Protect their network security with the latest and most efficient features and prevent intruders from unauthorised access.
- VI. Use the recent encryption standards to protect users' data and communication.
- VII. Install security software to inhibit access to illegal and inappropriate sites.
- VIII. Provide dispute resolution and robust customer support channels, such as channels and logs for feedback and complaints, which shall be accessible by NITDA and the FIRS.

- IX. All electronic data other than personal data, including users' records, access codes, logs, and invoice data, must be encrypted and stored or backed up on servers or data centres in Nigeria.

PART X

COMPLIANCE REQUIREMENTS

10.1 Quality of Service -NITDA shall have the authority to conduct investigations into the quality of service or the compliance of technology platforms provided by an Operator

10.2 Complaint Reporting—An Operator is obligated to address and resolve any consumer complaint within forty-eight (48) hours of receiving it. NITDA retains the discretion to investigate any complaint lodged by an end-user arising from the Operator's failure.

10.3 Assessment—As a compliance measure to ensure adherence to the stipulations of this framework and guideline, an assessment shall be conducted as determined by NITDA.

10.4 Reporting- Each Operator shall furnish NITDA with quarterly reports detailing its platform performance. Such reports shall be submitted electronically to the NITDA portal quarterly. Platform performance indices will include Security incidences, monthly average uptime, number of bug fixes monthly, number of technology patches and updates monthly, system failures, system upgrades, add-ons, records of customer support and user complaints,

10.5 Audit- NITDA reserves the right to audit all or a portion of the quality of service data obtained from an Operator. In discharging its duties, NITDA may modify the frequency of data collection, the subject services and parameters, network segments, and reporting intervals subject to audit.

10.6 Service Availability

- I. **Uptime Guarantee:** The Access Point Provider commits to an uptime of 99.9% per calendar month.
- II. **Maintenance:** Scheduled maintenance will be performed during off-peak hours, with 48-hour advance notice to the Client.

10.7 Performance Metrics for Service Providers

- I. **Invoice Processing:** Invoices will be processed and transmitted within 1 (24 Hours) business days from receipt.
- II. **Issue Resolution:** Any issues or errors in processing will be resolved within 2 (48 Hours) business days of notification.

- III. **Response Time:** Support requests will be acknowledged within 1 hour, resolved within 6 hours for critical issues, and within 1 (48-hour) business day for non-critical issues.
- IV. **Support Channels:** Support will be available through [e.g., email, phone, online portal].

PART XI

DISCONNECTION OF SERVICE PROVIDER

11.1 Guiding Principles

- I. NITDA shall be guided by the need to ensure that the interests of the affected Service Provider users are protected when approving an operator's disconnection.
- II. Other relevant issues that will guide the Agency's decision include the public interest in observing the rule of law and the need to entrench good corporate governance practices among Service Providers.

11.2 Pre-Disconnection Notice

- I. The Pre-Disconnection Notice to Access Point Providers shall be issued in all circumstances where NITDA has approved the disconnection of an Access Point Provider due to poor quality service or breach of these guidelines.
- II. Similarly, NITDA may issue a notice directing Users to onboard another System Integrator in the event of poor quality service, product failure, or a breach of these guidelines.
- III. Upon issuing such notice, NITDA shall, at its discretion, allow a grace period not exceeding twelve working days within which the Users would be at liberty to make arrangements to migrate to another Operator.
- IV. In every case where notice is given to an Operator, such notice shall include a directive to settle all the issues that resulted in the Provider's disconnection, failing which notice of the disconnection shall be published on the NITDA website.

11.3 Partial Disconnection

- I. Where NITDA approves the disconnection of an Access Point Provider, it reserves the right to authorise a partial disconnection on terms to be decided by NITDA.
- II. For these Guidelines, partial disconnection shall be limited to the disconnection of only outbound e-invoices from the sender Access Point Provider to the receiver Access Point Provider.
- III. The MBS platform shall provide data retrieval, archiving and transfer modalities for safekeeping and business continuity to ensure continuous availability.

PART XII

SANCTIONS, ENFORCEMENT AND COMPENSATION

12.1 Enforcement and Penalty

- I. Noncompliance with this regulation shall result in penalties, which include fines, remedial actions, disconnection of Service Provider operations, or other appropriate measures to be determined by NITDA.
- II. Individuals or entities affected by the Service Provider's product or operations or e-invoice actions or decisions shall have the right to seek legal remedies and compensation for any harm caused.

PART XIII MISCELLANEOUS

13.1 Review / Modification

- I. The NITDA may occasionally review or modify these Regulations, including the Schedules.
- II. In reviewing or modifying these Regulations, NITDA may request and receive advice or comments from external advisory groups whose advice is not binding on NITDA.
- III. The NITDA may, from time to time, issue additional rules, directives or guidelines on any aspect of these Regulations, which shall be of general application or specific to a Service Provider from time to time.

APPENDIX 1

OPERATOR GUIDELINES

A. Service Description for System Integrator

- a. The primary responsibility of a System Integrator is to integrate the business's internal systems, such as ERP systems, with the FIRS e-invoicing System. This involves mapping the relevant business processes and data fields to the e-invoice system schema to ensure data compatibility and accurate transmission in accordance with the Universal Business Language (UBL).
- b. **System Integrators are required to do the following:**
 - i. **ERP Compatibility:** Ensuring taxpayers' ERP systems and other financial management tools can generate invoices that meet the required format and standards. This includes customising or updating ERP configurations to meet technical specifications for eInvoicing.
 - ii. **Data Mapping:** Defining the data flow between the internal systems and the eInvoicing platform. Every invoice element (taxpayer details, transaction amounts, and VAT calculations) is correctly mapped to FIRS's standardised fields.
 - iii. **Secure Data Transmission:** Facilitating the safe transfer of eInvoices from the business's systems to FIRS through an Access Point Provider (APP). APPs act as intermediaries to validate and transmit e-invoice data. The System Integrator ensures seamless integration with the Access Point Providers and complies with security protocols, such as OAuth 2.0 authentication.
 - iv. **Troubleshooting and Monitoring:** System Integrators are responsible for continuously monitoring the data flow to ensure uninterrupted invoice submission. They troubleshoot issues related to data validation, system downtime, or transmission errors, ensuring that invoices are sent on time and comply with regulations.

c. **Legal and Technical Standards**

- i. Critical to the SI's role is ensuring that all systems comply with the technical and legal standards defined by e-invoicing regulations. This includes ensuring that invoices are transmitted and stored securely and include the necessary cryptographic features to prevent tampering.
- ii. **Digital Signature Implementation:** System Integrators must ensure that invoices generated are digitally signed using cryptographic techniques. This includes applying a cryptographic stamp identifier (CSID) and a digital signature to verify the invoice's authenticity. FIRS requires using the Elliptic Curve Digital Signature Algorithm (ECDSA) to ensure the integrity of eInvoices.
- iii. **Compliance with XAdES and PAdES Standards:** e Invoices must adhere to specific formats for electronic signatures, depending on whether they are in XML (Extensible Markup Language) or PDF/A-3 format. XML invoices must use XAdES (XML Advanced Electronic Signatures), while PDF invoices should comply with PAdES (PDF Advanced Electronic Signatures). System Integrators are responsible for implementing these formats to ensure that invoices are legally binding and verifiable.
- iv. **OAuth 2.0 Authentication:** To maintain secure communication between a taxpayer's ERP and the FIRS platform, the System Integrator must implement OAuth 2.0 authentication. This ensures that only authorised users and systems can interact with the platform, minimising the risk of unauthorised access or fraud. The Client ID and Secret Key generated during onboarding must be securely stored to prevent misuse.
- v. **Data Validation and Reporting:** System Integrators are also tasked with ensuring that the data submitted through the e-invoice system is valid and complies with data standards. This includes verifying that all mandatory fields are completed, ensuring accuracy in calculating taxes and VAT, and checking that the invoice follows the structure required.

d. **Cryptographic Security and Data Protection**

- i. Security is paramount in e-invoicing. The system integrator plays a significant role in ensuring secure communication between invoicing systems and FIRS using digital certificates and cryptographic signatures. Each invoice transmitted must be validated and stamped to maintain data integrity.
- ii. **Key Generation and Management:** System Integrators are responsible for generating and managing the public and private keys used in cryptographic stamping. Keys must be generated in compliance with FIPS 186 standards, and the private key used for signing invoices must be securely stored in a Hardware Security Module (HSM) or another secure method. Keys must be kept confidential, and any unauthorised export or use of keys must be strictly prohibited.
- iii. **Onboarding** – Digital Certificate Issuance and Renewal: The integration process involves requesting digital certificates for cryptographic stamps through the FIRS platform. The System Integrator must ensure that digital certificates are issued, installed, and renewed before expiration. Digital certificates validate the identity of the business sending the invoice and ensure that the invoice has not been altered after signing. This process involves generating and submitting One-Time Passwords (OTPs) for each device and managing Certificate Signing Requests (CSRs) to ensure each taxpayer's system is compliant.
- iv. **Certificate Revocation Management:** If a certificate is compromised, the System Integrator must revoke the digital certificate by submitting a revocation request through the FIRS platform. System Integrators are also responsible for monitoring the status of certificates through Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP) responders to ensure they remain valid.

e. **Error Handling and Troubleshooting**

System Integrators must develop robust processes for detecting and resolving errors that arise during invoice generation, validation, and transmission. The error-handling responsibilities include.

- i. **Validation Errors:** If an invoice fails validation due to missing data, incorrect formats, or non-compliance with FIRS regulations, the System Integrator must identify the error, correct it, and resubmit it. These validation processes ensure that businesses remain compliant and that all submitted invoices are processed correctly.
- ii. **System Downtime and Failures:** If the ERP system or eInvoicing platform experiences downtime, System Integrators must ensure that invoices can still be generated and stored until they can be submitted. This might involve creating offline storage systems or temporary solutions to manage invoice data.
- iii. **Real-Time Support:** System Integrators must provide real-time support to address issues as they arise, ensuring minimal disruption to business operations. This includes continuous monitoring of the system's health and performance, particularly during peak submission periods when businesses must submit multiple invoices simultaneously.

f. **Compliance Monitoring and Reporting**

i. **Ensuring ongoing compliance with the regulations**

The e-invoicing guidelines for UBL invoice format and the legal frameworks under Section 25, Part 5 of the Tax Administration and Enforcement Act 2007, which govern the e-invoice implementation, is, therefore, the core responsibility of the SI. System Integrators must:

- 1. **Monitor Compliance:** System Integrators monitor the system for compliance with FIRS guidelines and standards, ensuring that all invoices meet legal requirements. This includes ensuring that invoices are submitted in the correct format, that all necessary data fields are completed, and that the invoice is digitally signed.
- 2. **Auditing and Reporting:** System Integrators maintain audit logs of all invoices generated and transmitted to the FIRS platform. These logs provide evidence showing that the business complies with e-invoice regulations. System Integrators also create reports for both internal use and external audits by the FIRS.

3. **System Updates:** System Integrators are responsible for updating the integration to accommodate changes in FIRS regulations. This might involve adjusting data formats, updating encryption standards, or modifying workflows to comply with new tax rules.

Appendix 2

Standardised National Schema and Naming Conventions

A. Structure of Naming Convention

The e-invoicing system employs a standardised naming convention to ensure consistency, clarity, and ease of use across all aspects of invoice processing. By adhering to these conventions, users can streamline their operations, reduce errors, and maintain compliance with international standards.

B. Purpose of Naming Conventions

Naming conventions serve multiple purposes, including:

- **Standardisation:** Ensuring uniformity in naming across the system.
- **Clarity:** Making it easier to understand and locate specific invoices and related documents.
- **Compliance:** Meeting regulatory requirements and international standards.

C. Structure of Naming Conventions

- a. **Invoice Identifier:** Each invoice is assigned a unique code for tracking and referencing.
 - i. Format: INV[Sequential Number]
 - ii. Example: INV0001
- b. **Access Point Provider Identifier:** A unique code assigned to each Access Point Provider.
 - i. Format: Alphanumeric
 - ii. Example: B4B37F28
- c. **Time Stamp:** Based on the invoice's issued date.
 - i. Format: YYYYMMDD
 - ii. Example: 20240623

D. Importance of Naming Conventions

Naming conventions are vital for several reasons:

- **Efficiency:** Facilitates quick and accurate retrieval of invoices.

- **Data Integrity:** Prevents duplication and errors in invoice processing.
- **Regulatory Compliance:** Ensures adherence to national and international standards, such as the Harmonized System of Nomenclature (HSN).

E. Implementation Guidelines

- a. **Follow the Format:** Adhere strictly to the specified formats for each identifier.
- b. **Verify Accuracy:** Double-check codes and identifiers to ensure they are correct and up-to-date.
- c. **Consistent Application:** Apply naming conventions consistently across all documents and systems.
- d. By following these naming conventions, users can ensure their invoicing processes are streamlined, compliant, and efficient.

B. Adopted Standards for E-Invoicing in Nigeria

The Nigerian e-invoicing regulation adopts several international standards to enhance interoperability, security, and efficiency in the invoicing process. These standards ensure the system meets global best practices and regulatory requirements, facilitating smooth and reliable operations.

Key Standards Adopted

1. Harmonized System of Nomenclature (HSN) Codes

- a. **Purpose:** Standardizes the classification of goods for international trade.
- b. **Structure:** Six-digit codes, extendable by countries for more specific categorisation.
 - i. Example: '01' for live animals, '0101' for live horses, asses, mules, and hinnies, '010121' for purebred breeding horses.
- c. **Benefits:** Ensures uniform classification, simplifies customs procedures, aids in trade data analysis, and determines applicable tariffs and taxes.

2. ISO 27001/2022 (Information Security Management)

- a. **Purpose:** Provides a framework for managing information security.
- b. **Benefits:** Protects sensitive data, ensures compliance with security regulations, and mitigates risks associated with data breaches.

3. ISO 20022 (Financial Services Messaging)

- a. **Purpose:** Standardizes electronic data interchange between financial institutions.
- b. **Benefits:** Enhances the efficiency and interoperability of financial transactions, reduces errors, and facilitates regulatory compliance.

4. Universal Business Language (UBL)

- a. **Purpose:** Standardizes the format for electronic business documents.
- b. **Benefits:** Ensures compatibility with various e-commerce systems, reduces the need for custom integration, and supports global supply chain processes.

5. Implementation of Standards

- a. **System Integration:** Ensure the e-invoicing system is integrated with the above standards to maintain consistency and reliability.
- b. **Compliance Checks:** Regularly audit the system to verify compliance with the adopted standards.
- c. **Continuous Updates:** Stay informed about updates to these standards and implement changes promptly to remain compliant.

C. Harmonised System of Nomenclature (HSN) Code

The HSN Code (Harmonized System of Nomenclature) is an internationally recognised system for classifying goods. It was developed by the World Customs Organization (WCO) to facilitate the standardisation of trade and taxation globally. The HSN system helps systematically identify and classify goods for tax and customs purposes.

1. The HSN code consists of 6 to 8 digits:

- a. The first two digits represent the chapter under which the goods are classified (99 chapters).
- b. The following two digits represent the heading within the chapter.
- c. The following two digits represent the product category within the heading.

- d. Additional two digits (in some jurisdictions or industries) further classify local use.

2. Purpose:

- a. Used for the classification of goods in international trade.
- b. Facilitates the collection of accurate trade data and levying of tariffs and taxes.
- c. Helps streamline trade documentation and customs clearance.

3. Application:

- a. Import and Export: The HSN code is used globally in import and export documentation.
- b. GST (Goods and Services Tax): HSN codes are also used in indirect taxes to identify taxable goods and their applicable tax rates.
- c. Businesses and governments consistently classify products across borders and within tax regimes using standardised HSN codes.

4. Importance of HSN

- a. Verify Signed Invoice allows businesses to validate the authenticity and integrity of e-invoices issued by suppliers. This verification process confirms that the e-invoice has been digitally signed by the Federal Inland Revenue Service (FIRS) and has not been tampered with.
- b. Verify Signed Invoice allows businesses to validate the authenticity and integrity of e-invoices issued by suppliers. This verification process confirms that the e-invoice has been digitally signed by the Federal Inland Revenue Service (FIRS) and has not been tampered with.

5. Utilising the Global Standard

- a. The Merchant Buyer Solution allows businesses to generate and issue compliant customer invoices. However, before these invoices can be issued, businesses must first be enabled to invoice electronically on the MBS system by submitting the required information through the FIRS self-service portal.

- b. The Merchant Buyer Solution allows businesses to generate and issue compliant customer invoices. However, before these invoices can be issued, businesses must first be enabled to invoice electronically on the MBS system by submitting the required information through the FIRS self-service portal.

6. Requirements of HSN for E-Invoicing in Nigeria

- a. The Merchant Buyer Solution allows businesses to generate and issue compliant customer invoices. However, before these invoices can be issued, businesses must first be enabled to invoice electronically on the MBS system by submitting the required information through the FIRS self-service portal.
- b. Businesses can navigate to the IRN Validation section on this self-service portal to verify a signed invoice. This section will prompt the user to enter the Invoice Reference Number (IRN) assigned to the e-invoice by the MBS system.
- c. After inputting the IRN, the user clicks the 'Submit' button to initiate the verification process. The system then cross-checks the provided IRN against its database to validate the digital signature associated with the e-invoice.
- d. If the IRN is valid and matches the FIRS's records, the system will display a QR code, a green check mark, or a message indicating 'This is a Digitally Signed Invoice.' The QR code confirms that the e-invoice is authentic and has been digitally signed by the FIRS, guaranteeing its legitimacy and integrity.
- e. However, the system will display an appropriate error message if the provided IRN contains discrepancies or errors or if the digital signature verification fails. This could indicate that the e-invoice is invalid, has been tampered with, or has not been reported to the FIRS through the MBS platform.